

CIPHER KEY MANAGEMENT EQUIPMENT

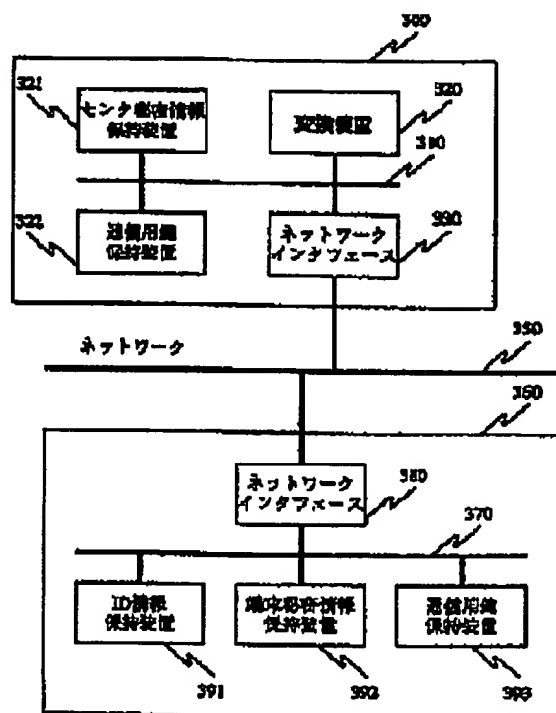
Patent number: JP8204702
Publication date: 1996-08-09
Inventor: MIYAUCHI HIROSHI
Applicant: NEC CORP
Classification:
- international: H04L9/32
- european:
Application number: JP19950013075 19950130
Priority number(s):

Report a data error here

Abstract of JP8204702

PURPOSE: To allow a center to conduct cipher communication with a terminal equipment and verification of the terminal equipment without having a cipher information list by writing an ID of a terminal equipment and cipher information in advance to the terminal equipment and to cipher data again and to obtain the cipher information at communication and to allow the center and the terminal equipment to use the cipher information in common.

CONSTITUTION: A center 300 keeps ciphering information Kc. The center 300 calculates terminal equipment cipher information $S_i = \text{Encipher}(Kc, ID_i)$ based on the ID_i of the terminal equipment to initialize the terminal equipment 360. The center 300 writes the ID_i and the S_i to the terminal equipment 360. At the start of cipher communication, an ID information storage device 391 of the terminal equipment 360 at first sends the ID_i to a network interface(IF) 380, the IF 380 sends the ID_i to a center 300 through a network 350. A terminal cipher information holding equipment sends information S_i to a key storage device 393. The center 300 receives the ID_i and gives it to a converter 320. The converter 320 receiving information Kc from a storage device 321 calculates the information S_i and stores it to a storage device 322. Thus, the center 300 and the terminal equipment 360 use the information S_i in common to allow the center 300 and the terminal equipment 360 to conduct cipher communication.



Data supplied from the esp@cenet database - Patent Abstracts of Japan

BEST AVAILABLE COPY

特開平8-204702

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-204702

(43) 公開日 平成8年(1996)8月9日

(51) IntCl ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/32				
// G09C 1/00		7259-5J		
			H04L 9/00	A

審査請求 有 請求項の数 4 O L (全 12 頁)

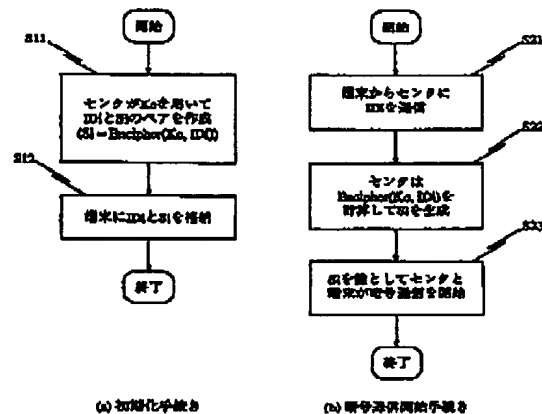
(21) 出願番号	特願平7-13075	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22) 出願日	平成7年(1995)1月30日	(72) 発明者	宮内 宏 東京都港区芝五丁目7番1号 日本電気株式会社内
		(74) 代理人	弁理士 京本 直樹 (外2名)

(54) 【発明の名称】 暗号鍵管理装置

(57) 【要約】

【目的】 センタが各端末の秘密情報リストをもたず、端末との秘密通信および端末認証を高速に行う。

【構成】 端末には、あらかじめ、端末のIDであるID_iと、端末秘密情報S_i=Encipher(K_e, ID_i) (K_eを鍵としてID_iを暗号化した結果)を書き込んでおく。ここでK_eはセンタが保持する秘密情報である。通信時には、センタは、上記の暗号化を再び行うことにより、S_iを得ることができるので、センタと端末でS_iを共有できる。



特開平8-204702

【特許請求の範囲】

【請求項1】 センタと複数の端末が暗号通信を行う際の暗号鍵管理装置であって、

前記センタにおいては、センタ秘密情報を保持する記憶手段と、暗号化および復号にあたって通信相手の端末のIDを受信するネットワークインタフェースと、該端末のIDを前記センタ秘密情報を用いて変換して通信用鍵を生成する変換装置と、該通信用鍵を保持する通信用鍵保持装置と、を具備し、

前記通信相手の端末においては、自己のIDを保持する装置と、該自己のIDを前記センタ秘密情報を用いて変換した結果である端末秘密情報を保持する記憶装置と、前記自己のIDを前記センタに送信するネットワークインタフェースと、該端末秘密情報を通信用の鍵として保持する装置と、を具備すること、

を特徴とする暗号鍵管理装置。

【請求項2】 センタと複数の端末が暗号通信を行う際の暗号鍵管理装置であって、

前記センタにおいては、少なくとも一つのセンタ秘密情報を保持する記憶手段と、暗号化および復号にあたって通信相手の端末のIDを受信し前記センタ秘密情報の中で通信に用いる識別番号を端末に送信するネットワークインタフェースと、識別番号を決定する装置と、前記端末のIDを前記識別番号に対応する前記センタ秘密情報を用いて変換して通信用鍵を生成する変換装置と、該通信用鍵を保持する通信用鍵保持装置と、を具備し、前記通信相手の端末においては、自己のIDを保持する装置と、該自己のIDを前記センタ秘密情報を用いて変換した結果である端末秘密情報のリストを保持する記憶装置と、前記自己のIDを前記センタに送信し、前記識別番号を受信するネットワークインタフェースと、前記識別番号に対応する端末秘密情報を通信用の鍵として保持する装置と、を具備すること、

を特徴とする暗号鍵管理装置。

【請求項3】 請求項1又は請求項2の暗号鍵管理装置において、前記端末IDから鍵を生成する変換として秘密鍵暗号を利用することを特徴とする暗号鍵管理装置。

【請求項4】 請求項1又は請求項2の暗号鍵管理装置において、前記端末IDから鍵を生成する変換としてハッシュ関数を利用することを特徴とする暗号鍵管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、サービスを提供するセンタと、サービスを受ける側が持つ端末の間の暗号通信および端末認証のための暗号鍵管理装置に関する。ここでいう端末は、移動端末やICカードなどを含む。また、端末として、プリペイドカードを用いることもできる。

【0002】

【従来の技術】 センタと端末で暗号化通信を行う場合、

通信に先立って暗号鍵の共有を行う必要がある。また、センタが端末認証を行う場合、その端末専用の秘密情報を端末側が持っていることを確認する。この場合には、秘密情報確認のための情報をセンタが持たなければならぬ。秘密情報確認のための情報は、秘密情報そのものであってもよい。公開鍵暗号系を用いれば、端末固有の公開鍵をセンタが保有する方法もあるが、ここでは秘密情報そのものをセンタが得る方法を中心に説明する。以下では、秘密鍵暗号系および公開鍵暗号系を用いる秘密鍵共有方法について説明するが、これらについては、「暗号と情報セキュリティ」(辻井、笠原著、昭晃堂、1990)に詳しく述べられている。以下では、本発明に直接関係する部分を説明する。

【0003】 秘密情報の共有(同一の秘密情報をセンタと端末がもつこと)のための、最も単純な方法として、あらかじめ端末毎に「端末ID」と「その端末用の鍵」のペアを設定し、端末はその端末の「IDと鍵」を保持し、センタはすべての端末の「IDと鍵」を保持する方法がある。すなわち、センタはすべての端末について「IDと鍵」のリストを持っている方法である。以下ではこの方法を「鍵リスト方式」と呼ぶ。

【0004】 鍵リスト方式では、暗号通信の際、端末IDを端末側から送信すれば、センタはリストからその端末用の暗号鍵を取り出せる。端末は自己の暗号鍵を保持しているので、両方で同一の鍵を共有できる。ここでは、秘密鍵のリストを持つ方法を述べたが、公開鍵リストを持ち、通信開始時に、『その通信に用いる臨時鍵』を公開鍵で暗号化して送る方法も知られている。いずれにしてもセンタは鍵のリストを持つ必要がある。

【0005】 公開鍵暗号系を応用する方法で、「IDによる鍵共有」の方法がある。この方法については、前記「暗号と情報セキュリティ」および特許明細書「暗号化方式」(特開昭63-314586)に詳しく述べられている。例えば、端末Aと端末Bが通信する場合を考え

る。端末Aは、自己の秘密情報 S_A と、共通の公開情報 α, n, e を保持している。端末AのID(識別番号)である ID_A は、

$$S_A^e \cdot ID_A \equiv 1 \pmod{n}$$

を満たすように決められる。同様に、端末Bは、自己の秘密情報 S_B と、共通の公開情報 α, n, e を保持しており、端末BのIDである ID_B は、

$$S_B^e \cdot ID_B \equiv 1 \pmod{n}$$

を満たす。AとBとが、通信を行う場合、 Λ は乱数 r_A を発生させ、

$$x_A = S_A \cdot \alpha^{r_A} \pmod{n}$$

なる x_A を計算する。AはBに ID_A, x_A を送る。同様にBは乱数 r_B を発生させ、

$$x_B = S_B \cdot \alpha^{r_B} \pmod{n}$$

なる x_B を計算し、 Λ に ID_B, x_B を送る。Aは、鍵 K_A を、

特開平8-204702

$$K_1 = (X_1^e \cdot ID_1)^{1/e} \pmod{n}$$

で計算し、Bは鍵 K_1 を

$$K_2 = (X_1^e \cdot ID_1)^{1/e} \pmod{n}$$

で計算する。すべての手続きが、正しく行われていれば、

$$K_1 = K_2 = \alpha^{x_1/m}$$

が成立し、鍵が共有される。

【0006】

【発明が解決しようとする課題】鍵リスト方式は、利用可能な端末の数が多くなると、リストが大きくなるという欠点を持っている。端末数が数万にも及ぶような場合、リストの検索に大きな計算量が必要になる。また、端末が増加する場合にそなえてリストの管理が必要になるが、この管理の手間も大きい。

【0007】IDによる鍵共有は、鍵リストを持つ必要がないため、鍵リスト方式が持っていた欠点は克服されている。しかし、IDによる鍵共有では、巾乗剰余演算($y = x^e \pmod{n}$)の形の演算)を利用するため、計算量が大きくなる。

【0008】本発明が解決しようとする課題は、鍵リストが不要で計算量も小さい鍵管理を実現するものである。

【0009】

【課題を解決するための手段】これらの課題を解決するため、本願の第一の発明は、センタと複数の端末が暗号通信を行う際の暗号鍵管理装置であって、前記センタにおいては、センタ秘密情報を保持する記憶手段と、暗号化および復号にあたって通信相手の端末のIDを受信するネットワークインタフェースと、該端末のIDを前記センタ秘密情報を用いて変換して通信用鍵を生成する変換装置と、該通信用鍵を保持する通信用鍵保持装置と、を具備し、前記通信相手の端末においては、自己のIDを保持する装置と、該自己のIDを前記センタ秘密情報を用いて変換した結果である端末秘密情報を保持する記憶装置と、前記自己のIDを前記センタに送信するネットワークインタフェースと、該端末秘密情報を通信用の鍵として保持する装置と、を具備すること、を特徴とする。

$$VM, K: Decipher(K, Encipher(K, M)) = M$$

【0016】という関係がある。ここで、Mは暗号化される対象文書、Kは鍵と呼ばれる。Encipher(K, M)は文書Mの鍵Kによる暗号化、Decipher(K, C)は暗号文Cの鍵Kによる復号を表す。暗号化関数Encipherは、暗号文 $C = Encipher(K, M)$ からKを知らずにMを復元すること、および文書MからKを知らずにCを作成することが困難になるように設計される。

【0017】本発明ではさらに、鍵つきハッシュ関数を用いる。鍵つきハッシュ関数は、 $C = hash(K, M)$

【0010】前述の課題を解決するため、本願の第二の発明は、センタと複数の端末が暗号通信を行う際の暗号鍵管理装置であって、前記センタにおいては、少なくとも一つのセンタ秘密情報を保持する記憶手段と、暗号化および復号にあたって通信相手の端末のIDを受信し前記センタ秘密情報の中で通信に用いる識別番号を端末に送信するネットワークインタフェースと、識別番号を決定する装置と、前記端末のIDを前記識別番号に対応する前記センタ秘密情報を用いて変換して通信用鍵を生成する変換装置と、該通信用鍵を保持する通信用鍵保持装置と、を具備し、前記通信相手の端末においては、自己のIDを保持する装置と、該自己のIDを前記センタ秘密情報を用いて変換した結果である端末秘密情報のリストを保持する記憶装置と、前記自己のIDを前記センタに送信し、前記識別番号を受信するネットワークインタフェースと、前記識別番号に対応する端末秘密情報を通信用の鍵として保持する装置と、を具備すること、を特徴とする。

【0011】前述の課題を解決するため、本願の第三の発明は、本願の第一又は第二の発明において、前記端末IDから鍵を生成する変換として秘密鍵暗号を利用することを特徴とする。

【0012】前述の課題を解決するため、本願の第四の発明は、本願の第一又は第二の発明において、前記端末IDから鍵を生成する変換としてハッシュ関数を利用することを特徴とする。

【0013】

【作用】本発明では、秘密鍵暗号を利用する。以下で述べる秘密鍵暗号の技術については、前記の「暗号と情報セキュリティ」に詳しく述べられている。ここでは、秘密鍵暗号を、本明細書での記号を用いて簡単に説明する。

【0014】秘密鍵暗号は、暗号化と復号で同一の鍵を使う方式である。暗号化関数Encipher、復号化関数Decipherの間には、

【0015】

【数1】

であり、Kを知らずにMからCを作成することが困難なものである。秘密鍵暗号との相違は、鍵つきハッシュ関数の場合は復号関数が存在しないことである。

【0018】以下、本発明の原理を説明する。

【0019】本発明では、センタのみが知る秘密情報Kをセンタが持ち、これを他に知られないように保持する。端末iを初期化する際に、端末に、その端末のIDであるID_iとその端末だけが持つ秘密情報S_iを格納する。ここで、S_iは、

$$S_i = Encipher(K, ID_i)$$

となるように定められる。S_iはセンタが計算し、端末

特開平8-204702

に書き込む。

【0020】センタと端末1とが通信を行う場合、センタは再び

$S_i = \text{Encipher}(K_c, ID_i)$

を計算して S_i を得る。端末は、 S_i を保持しているので、 S_i をセンタと端末で共有することができる。この方法を用いればセンタと端末1以外は S_i を計算することはできないため、秘密情報の共有が実現される。

【0021】

【実施例】次に本発明について図面を参照して詳細に説明する。

【0022】図1(a)は、本願の第一および第三、第四の発明におけるセンタおよび端末での初期化の処理の流れを表す図、図1(b)は、本願の第一および第三、第四の発明におけるセンタおよび端末での通信開始時の処理の流れを表す図、図7は本願の第一および第三、第四の発明の一実施例の構成を表す図である。以下これらの図に従って本願の第一および第三、第四の発明の実施例を説明する。

【0023】センタは、センタだけが持つ秘密情報 K_c を保持している。センタは、端末の初期化にあたってその端末のIDである ID_i から

$S_i = \text{Encipher}(K_c, ID_i)$

を計算する(図1ステップS11)。センタは ID_i と S_i を端末に書き込む(図1ステップS12)。ここで、センタは単一の装置である必要はない。複数のセンタが同一の秘密情報 K_c を保持しているような実施も可能である。

【0024】例えば、銀行のキャッシュカードに本発明を実施する場合、銀行の本店および各支店に K_c を持ち、どこの支店であっても正当な ID_i と S_i のペアを持つキャッシュカードを作成できるように実施できる。

【0025】端末の初期化時に暗号化関数でなく鍵つきハッシュ関数を用いる実施も可能である。

【0026】暗号通信の開始時には、まず端末360において、ID情報保持装置391が端末IDであるID_iをネットワークインタフェース380に送り、ネットワークインタフェース380はID_iをネットワーク350を介してセンタ300に送る(図1ステップS21)。また、端末秘密情報保持装置392は、端末秘密情報 S_i を通信用鍵保持装置393に送る。これら端末360内の通信はバス370を介して行われる。

【0027】センタ300においては、ネットワークインタフェース330がネットワーク350を介して端末360からID_iを受取り、変換装置320に送る。変換装置320は、センタ秘密情報保持装置321からセンタ秘密情報 K_c を受け取り、

$S_i = \text{Encipher}(K_c, ID_i)$

に従って端末秘密情報 S_i を計算し、通信用鍵保持装置322に格納する(図1ステップS22)。これらセン

タ300内の通信はバス310を介して行われる。端末は自己の秘密情報 S_i を保持しているから、以上の手続きで、センタおよび端末が秘密情報 S_i を共有できる。

以後、センタと端末は秘密通信を行うことができる(図1ステップS23)。センタは、また、 S_i を用いて端末認証を行うことも可能である。

【0028】端末初期化時にハッシュ関数を用いる実施の場合には、暗号通信開始時も同一のハッシュ関数を用いる。

【0029】暗号通信を行うセンタは、 K_c を保持していれば複数あってもよい。また、端末の初期化処理を行うセンタと同一であってもよいし、別個のものであってもよい。

【0030】銀行のキャッシュカードの例に戻ると、各キャッシュデイスペンサは K_c を保持し、キャッシュカードが挿入されると S_i を計算してカードの認証を行い、カードの正当性をチェックする。この場合、カードを発行する装置とキャッシュデイスペンサは異なる装置として実施することができる。すなわち、支店が持つカード発行装置は、カード発行専用であり、キャッシュデイスペンサはサービス供給専用になる。

【0031】図3は、本発明を利用するICカードリーダの一実施例である。

【0032】データ出力装置101は、カード検出装置103からデータ要求指令を受け取り、データ要求指令をICカード100に送る。データ出力装置101は、また、カウンタ110から端末IDを分別装置121から端末秘密情報を受け取り、端末IDおよび端末秘密情報をICカード100に送る。

【0033】データ入力装置102はカード検出装置103からの起動指令を受けて起動し、ICカード100から端末IDを受け取り、端末IDを暗号装置120へ送る。

【0034】カード検出装置103は、ICカード100の挿入を検出して、データ出力指令をRAM111に送り、RAM111からモード情報を受け取り、不揮発性メモリ112に出力指令を送る。カード検出装置103は、モード情報が「通信」の場合にはデータ出力装置101にデータ要求指令を、データ入力装置102に起動指令を送る。カード検出装置103は、モード情報が「書き込み」の場合には、カウンタ110に起動指令を送る。

【0035】モード設定インタフェース104は、利用者の入力を受け、モード情報をRAM111に送る。

【0036】カウンタ110は次に書き込むIDを保持している。カウンタ110は、カード検出装置103から出力指令を受けて起動し、カウンタ110が保持する数値を端末IDとして暗号装置120およびデータ出力装置101に送信し、カウンタ110が保持する数値に1を加える。

特開平8-204702

【0037】ID番号を供給する手段として、カウンタ以外に、入力インタフェースを介して入力する方法や、あらかじめ定められた関数で、順次IDをつくり出す方法をとることができる。

【0038】RAM111は、モード情報を保持する。ここで、モード情報は「通信」または「書き込み」である。RAM111は、モード設定インタフェースからモード情報を受け取り、これを保持する。RAM111は、カード検出装置103からデータ出力指令を受け取り、モード情報をカード検出装置103に送る。RAM111は、分別装置121からデータ出力指令を受け取り、モード情報を分別装置121に送る。

【0039】不揮発メモリ112は、センタ秘密情報を保持する。不揮発メモリ112は、カード検出装置103から出力指令を受けて、センタ秘密情報を暗号装置120へ送る。

【0040】通信鍵用RAM113は、分別装置121から通信鍵を受け取り保持する。通信鍵用RAM113は、ICカードとの通信を行う装置やICカードの認証を行う装置からアクセス可能に構成される。

【0041】暗号装置120は、カウンタ110から端末IDを不揮発性メモリ112からセンタ秘密情報を受け取り、センタ秘密情報を鍵として端末IDを暗号化して端末秘密情報を生成し、端末秘密情報を分別装置121に送る。暗号装置120は、また、データ入力装置102から端末IDを不揮発性メモリ112からセンタ秘密情報を受け取り、センタ秘密情報を鍵として端末IDを暗号化して端末秘密情報を生成し、端末秘密情報を分別装置121に送る。

【0042】分別装置121は、暗号装置120から端末秘密情報を受け取り、RAM111に出力指令を送り、RAM111からモード情報を受け取る。分別装置121は、モード情報が「通信」の場合には端末秘密情報を通信鍵用RAM113に送る。分別装置121は、モード情報が「書き込み」の場合には端末秘密情報をデータ出力装置101に送る。

【0043】ここでは、通信・書き込みの2つのモードを持つ装置として実施する例を示したが、通信だけを行う装置、書き込みだけを行う装置の実施も可能である。

【0044】図2(a)は、本願の第二および第三、第四の発明におけるセンタおよび端末での初期化の処理の流れを表す図、図2(b)は、本願の第二および第三、第四の発明におけるセンタおよび端末での通信開始時の処理の流れを表す図で、図8は本願の第二および第三、第四の発明の一実施例の構成を表す図である。以下これらの図に従って本願の第二および第三、第四の発明の実施例を説明する。

【0045】センタは、センタだけが持つ秘密情報 K_{ij} ($j=1, 2, \dots, n$)を保持している。センタは、端末の初期化にあたってその端末のIDであるID_iから

$S_{ij} = \text{Encipher}(K_{ij}, ID_i)$ ($j=1, 2, \dots, n$)

を計算する(図2ステップS111)。センタはID_iと S_{ij} ($j=1, 2, \dots, n$)を端末に書き込む(図2ステップS112)。ここで、センタは単一の装置である必要はない。複数のセンタが同一の秘密情報リスト K_{ij} ($j=1, 2, \dots, n$)を保持する実施も可能である。

【0046】暗号通信の開始時には、まず端末460において、ID情報保持装置491がID_iをネットワークインタフェース480に送る。ネットワークインタフェース480は受け取ったID_iをネットワーク450を介してセンタ400に送る(図2ステップS121)。

【0047】センタ400においては、ネットワークインタフェース430は、ネットワーク450を介して端末460からID_iを受け取る。ネットワークインタフェース430は、受け取ったID_iを変換装置420に送る。識別番号決定装置423はセンタ秘密情報保持装置421が保持する秘密情報のなかから一つを選ぶ(図2ステップS122)。この秘密情報の識別番号をjとする。識別番号決定装置423は、jをセンタ秘密情報保持装置421およびネットワークインタフェース430に送る。センタ秘密情報保持装置421は、少なくとも一つのセンタ秘密情報を保持する。センタ秘密情報保持装置421は、識別番号jを識別番号決定装置423から受け取り、jに対する秘密情報を変換装置420に送る。変換装置420は、ネットワークインタフェース430からID_iを、センタ秘密情報保持装置421からセンタ秘密情報 K_{ij} を受け取り、端末秘密情報 S_{ij} を $S_{ij} = \text{Encipher}(K_{ij}, ID_i)$ に従って計算する(図2ステップS122)。変換装置420は S_{ij} を通信用鍵保持装置422に格納する。ネットワークインタフェース430は、識別番号決定装置423から秘密情報識別番号jを受け取り、これをネットワーク450を介して端末460に送る(図2ステップS123)。センタ400内の通信はバス410を介して行われる。

【0048】端末460において、ネットワークインタフェース480がネットワーク460を介してセンタ400から識別番号jを受け取り、これを端末秘密情報保持装置492に送る。端末秘密情報保持装置492は、ネットワークインタフェース480から識別番号jを受け取り、jに対応する秘密情報 S_{ij} を通信用鍵保持装置493に格納する。端末460内の通信はバス470を介して行われる。

【0049】以上の手続きで、センタ400および端末460が秘密情報 S_{ij} を共有できる。以後、センタと端末は秘密通信を行うことができる(図2ステップS124)。センタは、また、 S_{ij} を用いて端末認証を行うことも可能である。

特開平8-204702

【0050】本実施例をキャッシュカードの例に適用すると、例えば、北海道地区のキャッシュデイスペンサーは K_{c1} を持ち、東北地区は K_{c2} を持つ、という方法で、地域毎に異なるセンタ秘密情報を利用することが可能となる。何らかの事情で、 K_{c1} が悪意の利用者に知られたとしても、その秘密情報を用いていない地域のサービスは安全に保たれる。秘密情報の利用区分は地域でなく、A銀行は K_{c1} 、B銀行は K_{c2} 、…という実施も可能である。また、時刻によって異なる秘密情報を用いる実施例も考えられる。

【0051】本実施例についても、暗号関数のかわりにハッシュ関数を用いることができる。

【0052】図4は、ICカード初期化の装置の一実施例である。

【0053】データ出力装置101aは、ID用カウンタ110aから端末IDを受け取りこれをICカード100aに送る。データ出力装置101aは、さらに、暗号装置120aから複数のセンタ秘密情報それぞれに対応する端末秘密情報を順次受け取り、ICカード100aに送る。

【0054】カード検出装置103aは、ID用カウンタ110aおよび秘密情報識別用カウンタ130に起動指令を送る。

【0055】ID用カウンタ110aは次に書き込むIDを保持している。ID用カウンタ110aは、カード検出装置103aから出力指令を受けて起動し、ID用カウンタ110aが保持する数値を端末IDとして暗号装置120aおよびデータ出力装置101aに送信し、ID用カウンタ110aが保持する数値に1を加える。

【0056】不揮発メモリ112aは、センタ秘密情報のリストを保持する。不揮発メモリ112aは、秘密情報識別用カウンタ130から秘密情報識別番号を受け取り、秘密情報識別番号に対応するセンタ秘密情報を暗号装置120aに送る。

【0057】暗号装置120は、カウンタ110aから端末IDを受け取り、不揮発性メモリ112からセンタ秘密情報を順次受け取り、各センタ秘密情報を鍵として端末IDを暗号化した端末秘密情報を生成し、端末秘密情報を順次データ出力装置101aに送る。

【0058】秘密情報識別用カウンタ130は、カード検出装置103aから起動指令を受け、不揮発性メモリ112aに格納されている秘密情報の識別番号を順次生成し、生成された識別番号を不揮発性メモリ112aに送る。

【0059】図5は、本発明をICカードリーダに適用する場合の一実施例である。

【0060】データ出力装置101bは、カード検出装置103bからデータ要求指令を受け取り、データ要求指令をICカード100bに送る。データ出力装置101bは、また、識別番号決定装置140から秘密情報識

別番号を受け取り、これをICカード100bに送る。

【0061】データ入力装置102bはカード検出装置103bからの起動指令を受けて起動し、ICカード100bから端末IDを受け取り、端末IDを暗号装置120bへ送る。

【0062】カード検出装置103bは、ICカード100bの挿入を検出して、データ出力カード検出装置103bは、データ出力装置101bにデータ要求指令を、データ入力装置102bに起動指令を、識別番号決定装置140に起動指令を送る。

【0063】不揮発メモリ112bは、少なくとも一つのセンタ秘密情報を保持する。不揮発メモリ112bは、識別番号決定装置140から秘密情報識別番号を受け取り、秘密情報識別番号に対応するセンタ秘密情報を暗号装置120bに送る。

【0064】通信鍵用RAM113bは、暗号装置120bから通信鍵を受け取り保持する。通信鍵用RAM113bは、ICカードとの通信を行う装置やICカードの認証を行う装置からアクセス可能に構成される。

【0065】暗号装置120bは、また、データ入力装置102bから端末IDを不揮発性メモリ112bからセンタ秘密情報を受け取り、センタ秘密情報を鍵として端末IDを暗号化して端末秘密情報を生成し、端末秘密情報を通信鍵用RAM113bに送る。

【0066】識別番号決定装置140は、カード検出装置103bからの起動指令を受けて起動し、不揮発性メモリ112bが保持するセンタ秘密情報のうちの一つを選択し、その識別番号を不揮発性メモリ112bおよびデータ出力装置101bに送る。

【0067】ここで、識別番号の決定は、乱数で行ってもよいし、時刻情報をもとにして行ってもよい。また、不揮発性メモリ112bが単一の秘密情報だけを持っている実施も可能であり、この場合、識別番号決定装置140は、不揮発性メモリ112bの持つ単一秘密情報の識別番号を出力することになる。

【0068】ここでは、通信・書き込みをそれぞれ独立の装置として実施する例を示したが、図3の実施例と同様に通信および書き込みのモードをもつ一つの装置としての実施も可能である。

【0069】図6はICカードを端末として本発明を実施する一例である。

【0070】出力装置200は、ID保持用不揮発性メモリ210から端末IDを受け取り、カードリーダ220に送る。

【0071】入力装置201は、カードリーダ220から、端末IDおよび端末秘密情報リストを受け取り、端末IDをID保持用不揮発性メモリ210に、端末秘密情報リストを秘密情報保持用不揮発性メモリ211に書き込む。

【0072】入力装置201はまた、カードリーダ22

特開平8-204702

0からデータ要求指令を受け取り、ID保持用不揮発性メモリ210に出力指令を送る。入力装置201はさらに、カードリーダー220から端末秘密情報識別番号を受け取り、これを秘密情報保持用不揮発性メモリ211に送る。

【0073】ID保持用不揮発性メモリ210は、入力装置201から端末IDを受け取り保持する。ID保持用不揮発性メモリ210は、また、入力装置201から出力指令を受け、端末IDを出力装置200に送る。

【0074】秘密情報保持用不揮発性メモリ211は、入力装置201から端末秘密情報リストを受け取り、保持する。秘密情報保持用不揮発性メモリ211は、また、入力装置201から端末秘密情報識別番号を受け取り、対応する端末秘密情報を通信経路RAM212に送る。

【0075】通信経路RAM212は、秘密情報保持用不揮発性メモリ211から、端末秘密情報を受け取り保持する。

【0076】通信経路RAM212は、カードリーダーとの通信を行う装置からアクセス可能に構成される。

【0077】ここでは、銀行のキャッシュカードに実施する例を述べたが、電話・交通手段など広い用途に用いられているプリペイドカードにも同様に実施することができる。また、スキーマ等で用いられている非接触型のICカードと料金徴収装置の間の通信に実施することもできる。

【0078】また、高速道路の料金徴収のため車載端末と路側装置の通信を行う方法への実施も可能である。この場合、車載端末をプリペイドカードとして実現する実施の他、車載端末の利用者を登録しておいて、後日料金を徴収する方法も考えられる。

【0079】

【発明の効果】本発明により、センタは各端末の秘密情報リストをもたずに、端末との秘密通信および端末認証を行うことができる。また、ID利用の鍵共有と異なり、高速な秘密鍵暗号やハッシュ関数を用いることが可能なため、大きな計算量は不要になった。

【図面の簡単な説明】

【図1】図1は、本願の第一および第三、第四の発明におけるセンタおよび端末における初期化時および通信開始時の処理の流れを示すフローチャートである。

【図2】図2は、本願の第二および第三、第四の発明におけるセンタおよび端末における初期化時および通信開始時の処理の流れを示すフローチャートである。

【図3】図3は、本願の第一の発明をカードリーダーに適用する実施例を表す図である。

【図4】図4は、本願の第二の発明のための初期化を行う装置の例を示す図である。

【図5】図5は、本願の第二の発明をカードリーダーに適用する実施例を表す図である。

05 【図6】図6は、本願の第二の発明をIDカードに適用する実施例を表す図である。

【図7】図7は、本願の第一の発明の実施例を表す図である。

10 【図8】図8は、本願の第二の発明の実施例を表す図である。

【符号の説明】

100, 100a, 100b ICカード

101, 101a, 101b データ出力装置

102, 102b データ入力装置

15 103, 103a, 103b カード検出装置

104 モード設定インタフェース

110 カウンタ

110a ID用カウンタ

111 RAM

20 112, 112a, 112b 不揮発性メモリ

113, 113b 通信経路RAM

120, 120a, 120b 暗号装置

121 分別装置

130 秘密情報識別用カウンタ

25 140 識別情報決定装置

200 出力装置

201 入力装置

210 ID保持用不揮発性メモリ

211 秘密情報保持用不揮発性メモリ

30 212 通信経路RAM

220 カードリーダー

300, 400 センタ

310, 410 バス

320, 420 変換装置

35 321, 421 センタ秘密情報保持装置

322, 422 通信経路保持装置

423 識別番号決定装置

330, 430 ネットワークインタフェース

350, 450 ネットワーク

40 360, 460 端末

370, 470 バス

380, 480 ネットワークインタフェース

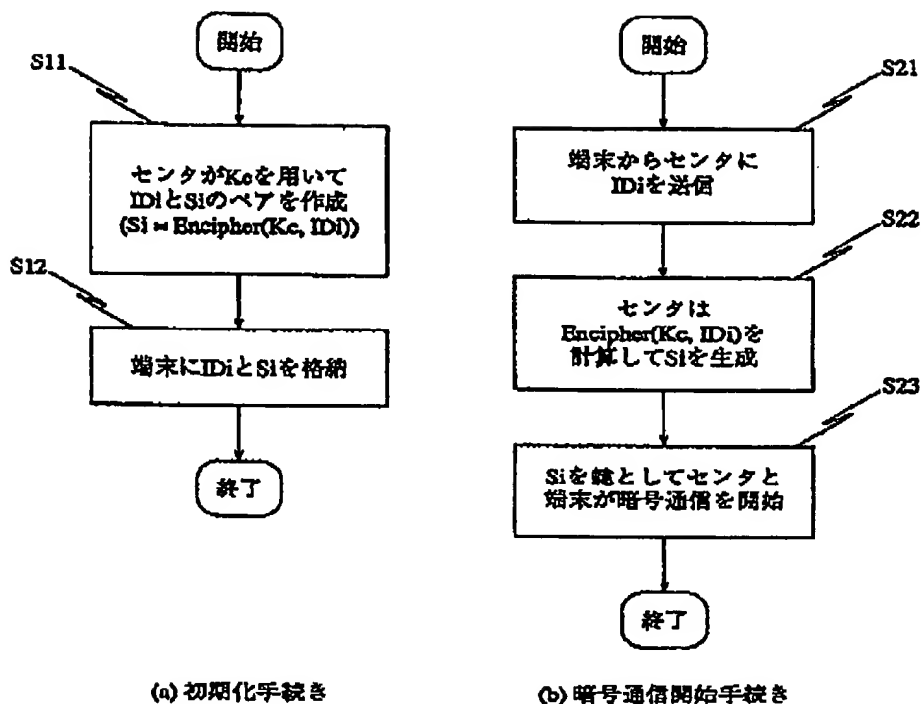
391, 491 ID情報保持装置

392, 492 端末秘密情報保持装置

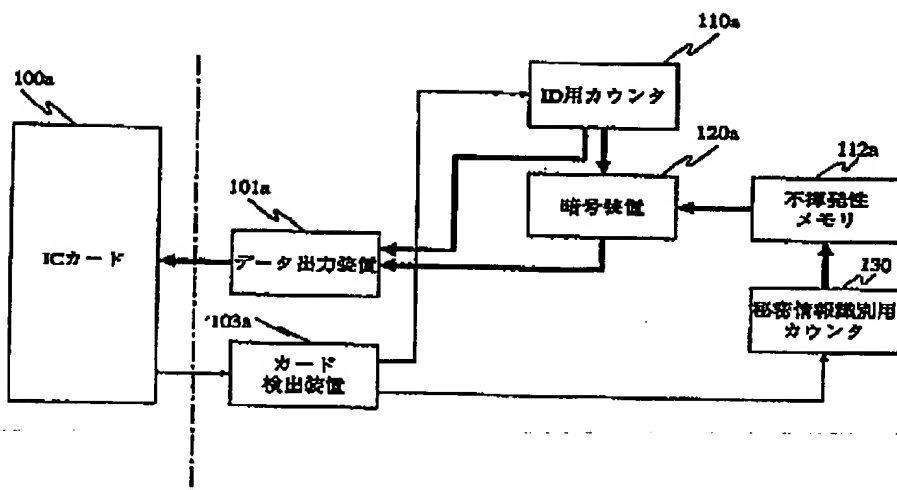
45 393, 493 通信経路保持装置

特開平8-204702

【図1】

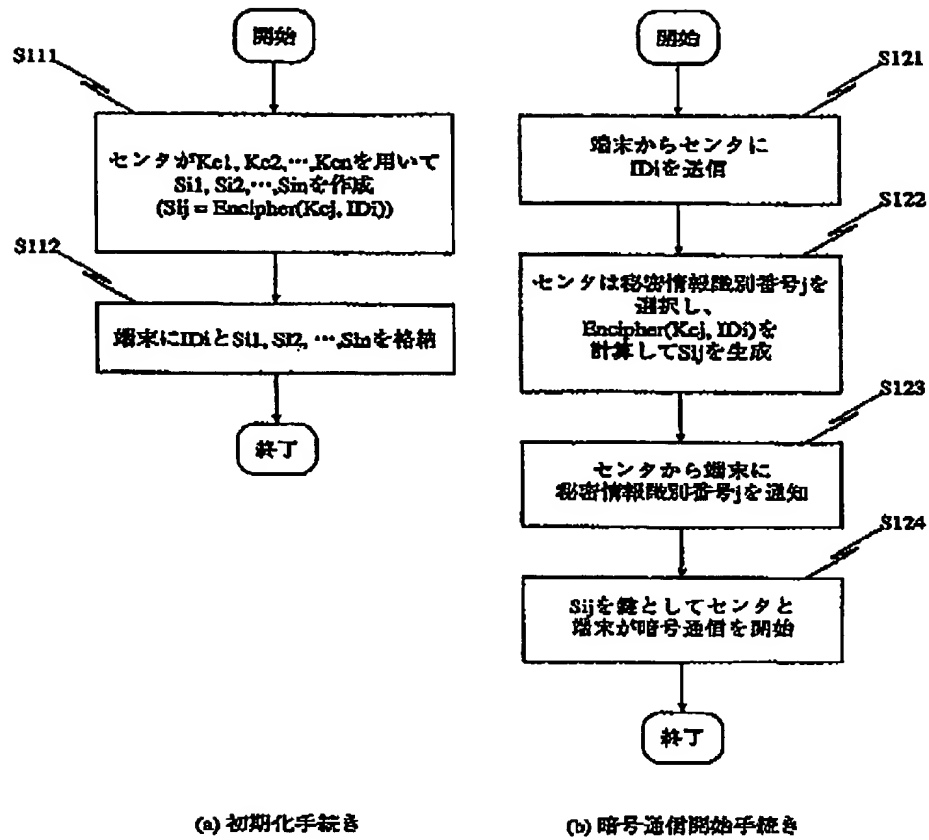


【図4】



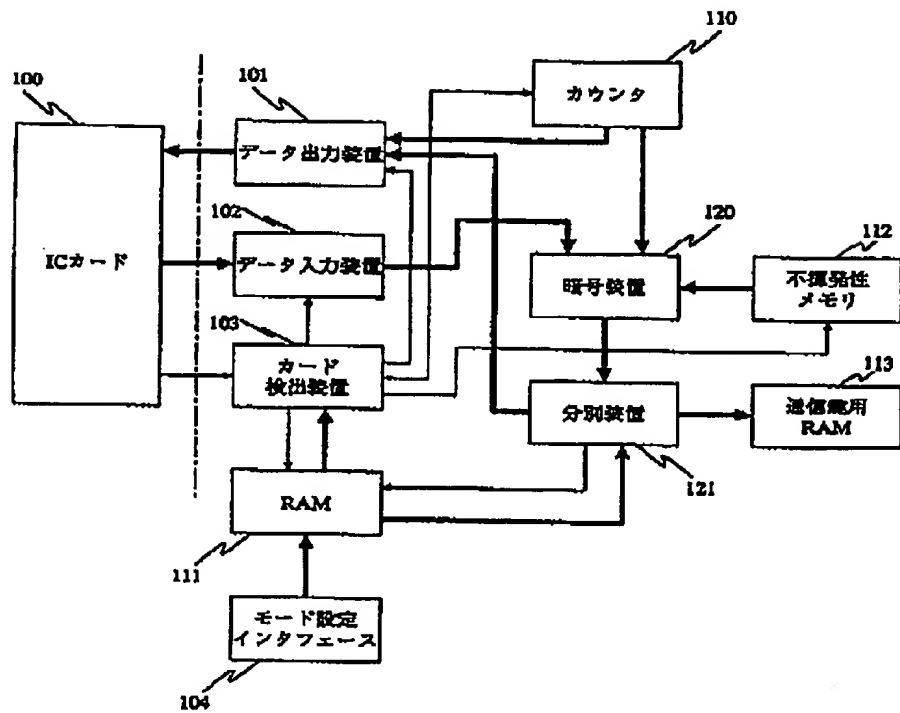
特開平8-204702

【図2】

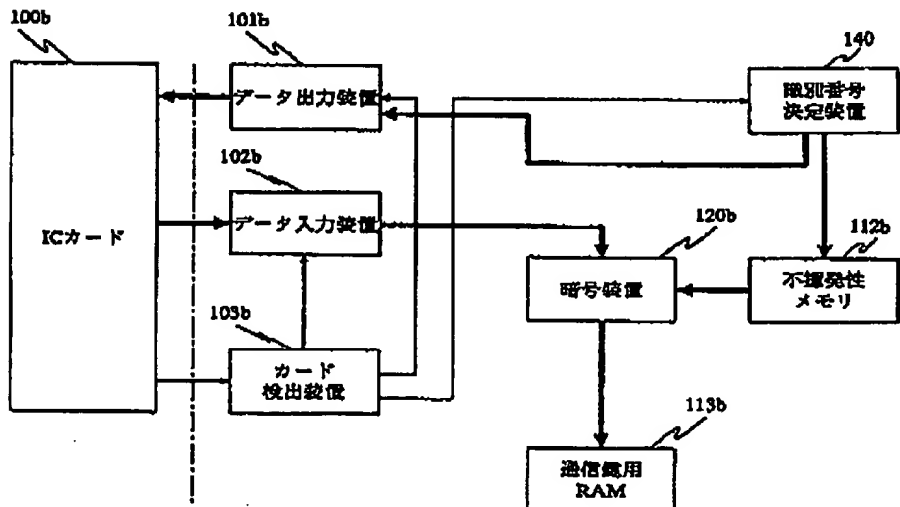


特開平8-204702

【図3】

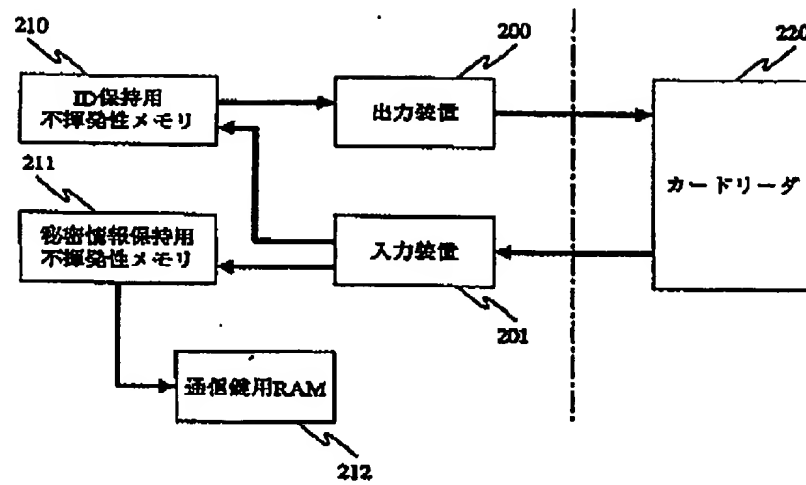


【図5】

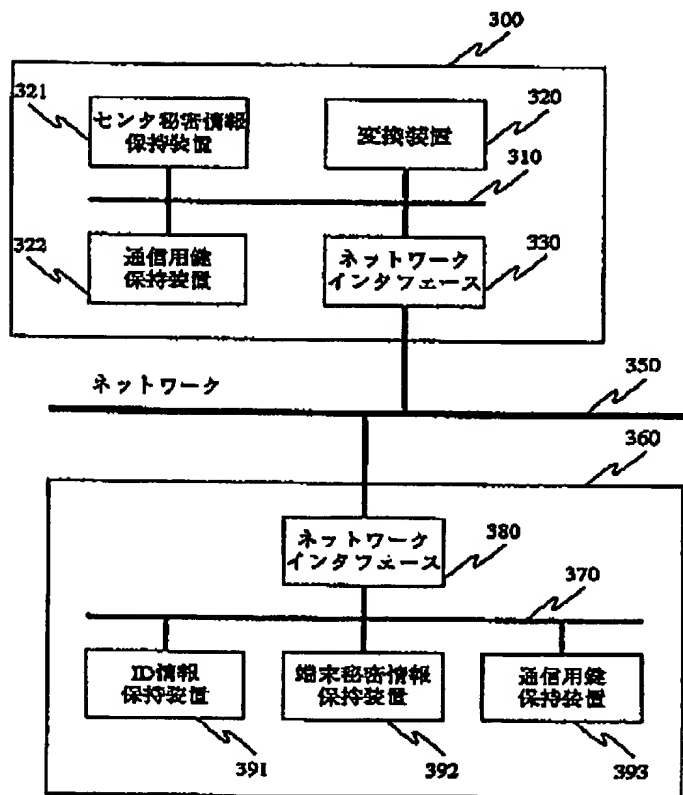


特開平8-204702

【図6】

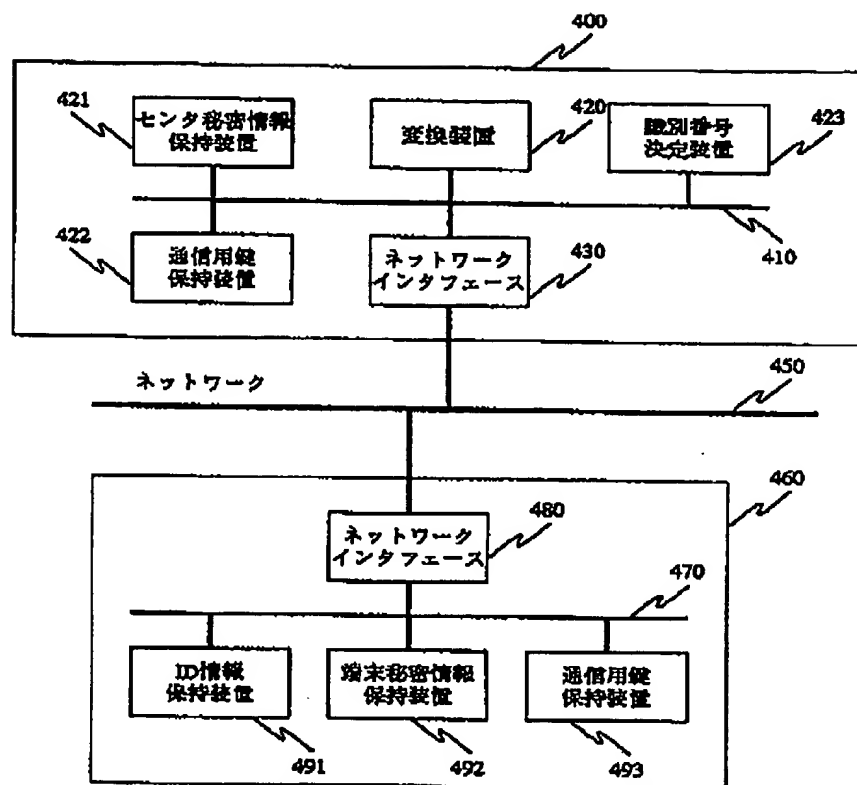


【図7】



特開平8-204702

【図8】



*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] Are cryptographic key management equipment at the time of a center and two or more terminals performing cryptocommunication, and it sets in said center. A storage means to hold center confidential information, and the network interface which receives ID of the terminal of a communications partner in encryption and decode, Provide the inverter which changes ID of this terminal using said center confidential information, and generates the key for a communication link, and the key supporting structure for a communication link holding this key for a communication link, and it sets to the terminal of said communications partner. The equipment holding self ID, and the storage holding the terminal confidential information which is the result of changing this self ID using said center confidential information, Cryptographic key management equipment characterized by providing the network interface which transmits said self ID to said center, and the equipment which holds this terminal confidential information as keys for a communication link.

[Claim 2] Are cryptographic key management equipment at the time of a center and two or more terminals performing cryptocommunication, and it sets in said center. A storage means to hold at least one center confidential information, and the network interface which transmits to a terminal the identification number which receives ID of the terminal of a communications partner in encryption and decode, and is used for a communication link in said center confidential information, The equipment which determines an identification number, and the inverter which changes ID of said terminal using said center confidential information corresponding to said identification number, and generates the key for a communication link, Provide the key supporting structure for a communication link holding this key for a communication link, and it sets to the terminal of said communications partner. The equipment holding self ID, and the storage holding the list of the terminal confidential information which is the result of changing this self ID using said center confidential information, Cryptographic key management equipment characterized by providing the network interface which transmits said self ID to said center, and receives said identification number, and the equipment which holds the terminal confidential information corresponding to said identification number as keys for a communication link.

[Claim 3] Cryptographic key management equipment characterized by using a secret key cryptosystem in the cryptographic key management equipment of claim 1 or claim 2 as conversion which generates a key from said terminal ID.

[Claim 4] Cryptographic key management equipment characterized by using a Hash Function in the cryptographic key management equipment of claim 1 or claim 2 as conversion which generates a key from said terminal ID.

[Translation done.]

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the cryptographic key management equipment for the cryptocommunication between the center which offers service, and the terminal which the side which receives service has, and terminal authentication. A terminal here contains a migration terminal, an IC card, etc. Moreover, a PURIPEDO card can also be used as a terminal.

[0002]

[Description of the Prior Art] When a center and a terminal perform an encryption communication link, it is necessary to share a cryptographic key in advance of a communication link. Moreover, when a center performs terminal authentication, it checks that the terminal side has the confidential information only for the terminals. In this case, a center must have the information for a confidential information check. The information for a confidential information check may be the confidential information itself. Although there is also an approach a center holds the public key of a terminal proper if a public-key-encryption system is used, it explains focusing on the approach a center obtains the confidential information itself here. Although the private key share approach of using a secret key cryptosystem system and a public-key-encryption system is explained below, these are stated to "the code and the information security" (Tsujii, the Kasahara work, Shokodo, 1990) in detail. Below, the part related to this invention is explained directly.

[0003] As simplest approach for sharing (a center and a terminal should have the same confidential information) of confidential information, the pair of "Terminal ID" and "the key for the terminals" is beforehand set up for every terminal, a terminal holds "ID and the key" of the terminal, and a center has a method of holding "ID and the key" of all terminals. That is, a center is an approach which has a list of "ID and keys" about all terminals. Below, this approach is called a "key list mode."

[0004] In a key list mode, if Terminal ID is transmitted from a terminal side in the case of cryptocommunication, a center can take out the cryptographic key for the terminals from a list. Since the terminal holds the self cryptographic key, the same key is sharable by both. Here, although the approach with the list of private keys was described, it has a public key list and the method of enciphering and sending "the extraordinary key used only within the communication link" with a public key at the time of communication link initiation is also learned. Anyway, a center needs to have a list of keys.

[0005] There is an approach "key shared [by ID]" by the approach of applying a public-key-encryption system. This approach is stated to the above "a code and an information security" and a patent specification "a cipher system" (JP,63-314586,A) in detail. For example, the case where Terminal A and Terminal B communicate is considered. Terminal A is the self confidential information SA. The common public information alpha, n, and e is held. IDA which is ID (identification number) of Terminal A SA e and $IDA \cdot e \pmod n$

***** -- it is decided like. Similarly, Terminal B is the self confidential information SB. IDB which the common public information alpha, n, and e is held, and is ID of Terminal B SB e and $IDB \cdot e \pmod n$

*****. When A and B communicate, A is a random number rA. It is made to generate and they are $x_A = SA$ and $\alpha_A \pmod n$.

Becoming x_A It calculates. A is IDA and x_A to B. It sends. B is a random number rB similarly. It is made to generate and they are $x_B = SB$ and $\alpha_B \pmod n$.

Becoming x_B It calculates and they are IDB and x_B to A. It sends. A is Key KA. $KA = (x_B \cdot e \text{ and } IDB) \cdot r_A \pmod n$

Coming out and calculating, B is Key KB. $KB = (XA^e \text{ and } IDA) \cdot rB \pmod{n}$

It comes out and calculates. If all procedure is performed correctly, $KA = KB = \alpha^a r^B$ will be materialized and a key will be shared.

[0006]

[Problem(s) to be Solved by the Invention] The key list mode has the fault that a list becomes large, if the number of available terminals increases. When the number of terminals also attains to tens of thousands, big computational complexity is needed for retrieval of a list. Moreover, although it offers when a terminal increases, and management of a list is needed, the time and effort of this management is also large.

[0007] Since the key share by ID does not need to have a key list, the fault which the key list mode had is conquered. However, in the key share by ID, in order to use an exponentiation remainder operation (operation of the form of $y = xe \pmod{n}$), computational complexity becomes large.

[0008] The technical problem which this invention tends to solve has an unnecessary key list, and computational complexity also realizes small key management.

[0009]

[Means for Solving the Problem] In order to solve these technical problems, invention of the first of this application Are cryptographic key management equipment at the time of a center and two or more terminals performing cryptocommunication, and it sets in said center. A storage means to hold center confidential information, and the network interface which receives ID of the terminal of a communications partner in encryption and decode, Provide the inverter which changes ID of this terminal using said center confidential information, and generates the key for a communication link, and the key supporting structure for a communication link holding this key for a communication link, and it sets to the terminal of said communications partner. The equipment holding self ID, and the storage holding the terminal confidential information which is the result of changing this self ID using said center confidential information, It is characterized by providing the network interface which transmits said self ID to said center, and the equipment which holds this terminal confidential information as keys for a communication link.

[0010] In order to solve the above-mentioned technical problem, invention of the second of this application Are cryptographic key management equipment at the time of a center and two or more terminals performing cryptocommunication, and it sets in said center. A storage means to hold at least one center confidential information, and the network interface which transmits to a terminal the identification number which receives ID of the terminal of a communications partner in encryption and decode, and is used for a communication link in said center confidential information, The equipment which determines an identification number, and the inverter which changes ID of said terminal using said center confidential information corresponding to said identification number, and generates the key for a communication link, Provide the key supporting structure for a communication link holding this key for a communication link, and it sets to the terminal of said communications partner. The equipment holding self ID, and the storage holding the list of the terminal confidential information which is the result of changing this self ID using said center confidential information, Said self ID is transmitted to said center, and it is characterized by providing the network interface which receives said identification number, and the equipment which holds the terminal confidential information corresponding to said identification number as keys for a communication link.

[0011] In order to solve the above-mentioned technical problem, invention of the third of this application is characterized by using a secret key cryptosystem as conversion which generates a key from said terminal ID in the first of this application, or the second invention.

[0012] In order to solve the above-mentioned technical problem, invention of the fourth of this application is characterized by using a Hash Function as conversion which generates a key from said terminal ID in the first of this application, or the second invention.

[0013]

[Function] A secret key cryptosystem is used in this invention. The technique of the secret key cryptosystem described below is stated to the aforementioned "aforementioned code and information security" in detail. Here, a secret key cryptosystem is briefly explained using the notation in this specification.

[0014] A secret key cryptosystem is a method using the same key in encryption and decode. Between the encryption function Encipher and the decryption function Decipher, it is [0015].

[Equation 1]

$$\forall M, K : \text{Decipher}(K, \text{Encipher}(K, M)) = M$$

[0016] There is relation to say. Here, the object document and K as which M is enciphered are called a key. Encryption according [Encipher (K, M)] to the key K of Document M and Decipher (K, C) express the decode with the key K of Cipher C. From restoring M for cipher $C = \text{Encipher}(K, M)$ to K to not knowing, and Document M, in K, the encryption function Encipher is designed so that it may become difficult to create C to not knowing.

[0017] In this invention, a Hash Function with a key is used further. The Hash Function with a key is $C = \text{hash}(K, M)$.

It is difficult to come out, to be and to create C for K from M to not knowing. In the case of a Hash Function with a key, the difference with a secret key cryptosystem is that a decode function does not exist.

[0018] Hereafter, the principle of this invention is explained.

[0019] Confidential information Kc which only a center gets to know in this invention A center has, and this is held so that it otherwise may not be known. IDi which is ID of the terminal at a terminal in case Terminal i is initialized Confidential information Si which only the terminal has It stores. Here, it is Si. $Si = \text{Encipher}(Kc \text{ and } IDi)$

It is determined that it becomes. Si A center calculates and it writes in a terminal.

[0020] When a center and Terminal i communicate, a center is $Si = \text{Encipher}(Kc \text{ and } IDi)$ again.

It calculates and is Si. It obtains. A terminal is Si. Since it holds, it is Si. It is sharable by the center and the terminal. If this approach is used, it will be Si except a center and Terminal i. Since it is incalculable, sharing of confidential information is realized.

[0021]

[Example] Next, this invention is explained to a detail with reference to a drawing.

[0022] Drawing where drawing and drawing 1 (b) to which drawing 1 (a) expresses the flow of processing of initialization with the center and terminal in the first and the third and fourth invention of this application express the flow of the processing at the time of communication link initiation with the center and terminal in the first and the third and fourth invention of this application, and drawing 7 are drawings showing the configuration of one example of the first of this application, and the third and the fourth invention. According to these drawings, the example of the first of this application, and the third and the fourth invention is explained below.

[0023] A center is the confidential information Kc which only a center has. It holds. IDi whose center is ID of the terminal in initialization of a terminal from -- $Si = \text{Encipher}(Kc \text{ and } IDi)$

It calculates (drawing 1 step S11). A center is IDi. Si It writes in a terminal (drawing 1 step S12). Here, a center does not need to be single equipment. Confidential information Kc with two or more same centers Operation which is held is also possible.

[0024] For example, when carrying out this invention to the ATM card of a bank, it is Kc to the head office and each branch of a bank. It is just IDi, even if it has and is a branch of what. Si It can carry out so that an ATM card with a pair can be created.

[0025] The operation which uses not an encryption function but a Hash Function with a key at the time of initialization of a terminal is also possible.

[0026] IDi whose ID information supporting structure 391 is [in / in the time of initiation of cryptocommunication / a terminal 360] Terminal ID first Delivery and a network interface 380 are IDi to a network interface 380. It sends to a center 300 through a network 350 (drawing 1 step S21). Moreover, the terminal confidential information supporting structure 392 is the terminal confidential information Si. It sends to the key supporting structure 393 for a communication link. The communication link within these terminals 360 is performed through a bus 370.

[0027] In a center 300, a network interface 330 minds a network 350, and it is IDi from a terminal 360. It sends to a receipt and an inverter 320. An inverter 320 is the center confidential information supporting structure 321 to the center confidential information Kc. Reception, $Si = \text{Encipher}(Kc \text{ and } IDi)$

It is alike, it follows and is the terminal confidential information Si. It calculates and stores in the key supporting structure 322 for a communication link (drawing 1 step S22). The communication link in these centers 300 is performed through a bus 310. A terminal is the self confidential information Si. Since it holds, a center and a terminal are confidential information Si by the above procedure. It is sharable. Henceforth, a center

and a terminal can perform secret communication (R> drawing 1 1 step S23). A center is Si again. It is also possible to use and to perform terminal authentication.

[0028] In the operation which uses a Hash Function at the time of terminal initialization, the Hash Function same also at the time of cryptocommunication initiation is used.

[0029] The center which performs cryptocommunication is Kc. As long as it holds, there may be more than one. Moreover, it may be the same as that of the center which performs initialization processing of a terminal, and may be separate.

[0030] If it returns to the example of the ATM card of a bank, each cash dispenser is Kc. It is Si, if it holds and an ATM card is inserted. It calculates, a card is attested and the justification of a card is checked. In this case, the equipment which publishes a card, and a cash dispenser can be carried out as different equipment. Namely, the card issue equipment which a branch has is exclusively for card issue, and a cash dispenser becomes service supplies only.

[0031] Drawing 3 is one example of IC card reader using this invention.

[0032] Data output equipment 101 sends reception and a data demand command for a data demand command to IC card 100 from card detection equipment 103. Data output equipment 101 sends [judgment equipment 121 to terminal confidential information] Terminal ID for reception, Terminal ID, and terminal confidential information to IC card 100 from a counter 110 again.

[0033] A data entry unit 102 is started in response to the starting command from card detection equipment 103, and Terminal ID is sent to reception from IC card 100, and it sends Terminal ID to data encryption equipment 120.

[0034] Card detection equipment 103 detects insertion of IC card 100, and mode information is sent to RAM111 from delivery and RAM111, and it sends an output command for a data output command to reception and nonvolatile memory 112. A data demand command is sent to data output equipment 101, and card detection equipment 103 sends a starting command to a data entry unit 102, when mode information is "a communication link." Card detection equipment 103 sends a starting command to a counter 110, when mode information is "writing."

[0035] The mode setting interface 104 receives a user's input, and sends mode information to RAM111.

[0036] The counter 110 holds ID written in a degree. A counter 110 starts in response to an output command from card detection equipment 103, it transmits to data encryption equipment 120 and data output equipment 101 by using as Terminal ID the numeric value which a counter 110 holds, and 1 is added to the numeric value which a counter 110 holds.

[0037] The approach of inputting through an input interface as a means to supply an ID number, in addition to a counter, and the approach of making ID one by one with the function defined beforehand can be taken.

[0038] RAM111 holds mode information. Here, mode information is "a communication link" or "writing." RAM111 holds reception and this for mode information from a mode setting interface. RAM111 sends a data output command to reception from card detection equipment 103, and sends mode information to card detection equipment 103. RAM111 sends a data output command to reception from judgment equipment 121, and sends mode information to judgment equipment 121.

[0039] Nonvolatile memory 112 holds center confidential information. Nonvolatile memory 112 sends center confidential information to data encryption equipment 120 in response to an output command from card detection equipment 103.

[0040] RAM113 for communication link keys carries out reception maintenance of the communication link key from judgment equipment 121. RAM113 for communication link keys consists of equipment which performs the communication link with an IC card, and equipment which performs authentication of an IC card accessible.

[0041] It uses [nonvolatile memory / 112] center confidential information as a key for Terminal ID by using center confidential information as reception from a counter 110, and data encryption equipment 120 enciphers Terminal ID, generates terminal confidential information, and sends terminal confidential information to judgment equipment 121. It uses [nonvolatile memory / 112] center confidential information as a key for Terminal ID by using center confidential information as reception from a data entry unit 102 again, and data encryption equipment 120 enciphers Terminal ID, generates terminal confidential information, and sends terminal confidential information to judgment equipment 121.

[0042] Judgment equipment 121 receives [terminal confidential information] RAM111 to delivery and mode information from data encryption equipment 120 for an output command to reception and RAM111. Judgment equipment 121 sends terminal confidential information to RAM113 for communication link keys, when mode information is "a communication link." Judgment equipment 121 sends terminal confidential information to data output equipment 101, when mode information is "writing."

[0043] Although the example here carried out as equipment with the two modes of a communication link and writing was shown, operation of the equipment which only communicates, and the equipment which performs only writing is also possible.

[0044] Drawing and drawing 2 (b) to which drawing 2 (a) expresses the flow of processing of initialization with the second and third, and fourth center and terminal in invention of this application are drawing showing the flow of the processing at the time of communication link initiation with the second and third, and fourth center and terminal in invention of this application, and drawing 8 is the second of this application and the third, and drawing showing the fourth configuration of one example of invention. According to these drawings, the example of the second of this application and the third, and the fourth invention is explained below.

[0045] The center holds the confidential information Kcj ($j = 1, 2, \dots, n$) which only a center has. IDi whose center is ID of the terminal in initialization of a terminal from -- $Sij = \text{Encipher}(Kcj \text{ and } IDi)$ ($j = 1, 2, \dots, n$) It calculates (drawing 2 step S111). A center is IDi. Sij ($j = 1, 2, \dots, n$) is written in a terminal (drawing 2 step S112). Here, a center does not need to be single equipment. Operation holding the confidential information list Kcj ($j = 1, 2, \dots, n$) with two or more same centers is also possible.

[0046] At the time of initiation of cryptocommunication, it sets to a terminal 460 first, and ID information supporting structure 491 is IDi. It sends to a network interface 480. A network interface 480 is received IDi. It sends to a center 400 through a network 450 (drawing 2 step S121).

[0047] In a center 400, a network interface 430 minds a network 450, and it is IDi from a terminal 460. It receives. A network interface 430 is received IDi. It sends to an inverter 420. Identification number decision equipment 423 chooses one from the confidential information which the center confidential information supporting structure 421 holds ($R > \text{drawing 2 2 step S122}$). The identification number of this confidential information is set to j. Identification number decision equipment 423 sends j to the center confidential information supporting structure 421 and a network interface 430. The center confidential information supporting structure 421 holds at least one center confidential information. The center confidential information supporting structure 421 sends confidential information [as opposed to reception and j for an identification number j] to an inverter 420 from identification number decision equipment 423. An inverter 420 is a network interface 430 to IDi. They are reception and the terminal confidential information Sij about the center confidential information supporting structure 421 to the center confidential information Kcj $Sij = \text{Encipher}(Kcj \text{ and } IDi)$

It is alike, and follows and calculates (drawing 2 step S122). An inverter 420 stores Sij in the key supporting structure 422 for a communication link. Reception is minded for the confidential information identification number j from identification number decision equipment 423, it minds a network 450 for this, and a network interface 430 sends it to a terminal 460 (drawing 2 step S123). The communication link in a center 400 is performed through a bus 410.

[0048] In a terminal 460, through a network 460, an identification number j is sent to reception from a center 400, and a network interface 480 sends this to the terminal confidential information supporting structure 492. The terminal confidential information supporting structure 492 stores the confidential information Sij corresponding to reception and j for an identification number j in the key supporting structure 493 for a communication link from a network interface 480. The communication link within a terminal 460 is performed through a bus 470.

[0049] A center 400 and a terminal 460 can share confidential information Sij between the above procedure. Henceforth, a center and a terminal can perform secret communication (drawing 2 step S124). A center can also perform terminal authentication again using Sij .

[0050] If this example is applied to the example of an ATM card, it will be the approach the cash dispenser in the Hokkaido area has Kc1, and a northeast area has Kc2, and it will become possible to use different center confidential information for every area, for example. Even if Kcj is known for a certain situation by the malicious user, service of the area which does not use the confidential information is maintained at insurance.

Not an area but A bank of the use partition of confidential information is possible also for the operation [bank / Kc1 and / B] Kc2 and --. Moreover, the example using the confidential information which changes with time of day is also considered.

[0051] Also about this example, a Hash Function can be used instead of a code function.

[0052] Drawing 4 is one example of the equipment of IC card initialization.

[0053] Data output equipment 101a receives Terminal ID from counter 110 for ID a, and sends this to IC card 100a. Data output equipment 101a sends the terminal confidential information corresponding to two or more center confidential information of each to reception and IC card 100a one by one from data-encryption-equipment 120a further.

[0054] Card detection equipment 103a sends a starting command to counter 110 for ID a, and the counter 130 for confidential information discernment.

[0055] Counter 110a for ID holds ID written in a degree. Counter 110a for ID is started in response to an output command from card detection equipment 103a, transmits to data-encryption-equipment 120a and data output equipment 101a by using as Terminal ID the numeric value which counter 110a for ID holds, and adds 1 to the numeric value which counter 110a for ID holds.

[0056] Nonvolatile memory 112a holds the list of center confidential information. Nonvolatile memory 112a sends the center confidential information corresponding to reception and a confidential information identification number for a confidential information identification number to data-encryption-equipment 120a from the counter 130 for confidential information discernment.

[0057] Data encryption equipment 120 generates the terminal confidential information which used [Terminal ID] reception and each center confidential information as the key for nonvolatile memory 112 to reception and center confidential information one by one from counter 110a, and enciphered Terminal ID, and sends terminal confidential information to data output equipment 101a one by one.

[0058] The counter 130 for confidential information discernment receives a starting command from card detection equipment 103a, carries out sequential generation of the identification number of the confidential information stored in nonvolatile memory 112a, and sends the generated identification number to nonvolatile memory 112a.

[0059] Drawing 5 is one example in the case of applying this invention to IC card reader.

[0060] Data output equipment 101b sends reception and a data demand command for a data demand command to IC card 100b from card detection equipment 103b. Data output equipment 101b sends a confidential information identification number to reception from identification number decision equipment 140, and sends this to IC card 100b.

[0061] Data entry unit 102b is started in response to the starting command from card detection equipment 103b, and Terminal ID is sent to reception from IC card 100b, and it sends Terminal ID to data-encryption-equipment 120b.

[0062] card detection equipment 103b -- insertion of IC card 100b -- detecting -- data output card detection equipment 103b -- a starting command is sent to data entry unit 102b, and a starting command is sent for a data demand command to identification number decision equipment 140 at data output equipment 101b.

[0063] Nonvolatile memory 112b holds at least one center confidential information. Nonvolatile memory 112b sends the center confidential information corresponding to reception and a confidential information identification number for a confidential information identification number to data-encryption-equipment 120b from identification number decision equipment 140.

[0064] RAM 113b for communication link keys carries out reception maintenance of the communication link key from data-encryption-equipment 120b. RAM 113b for communication link keys consists of equipment which performs the communication link with an IC card, and equipment which performs authentication of an IC card accessible.

[0065] It uses [b / nonvolatile memory 112] center confidential information as a key for Terminal ID by using center confidential information as reception from data entry unit 102b again, and data-encryption-equipment 120b enciphers Terminal ID, generates terminal confidential information, and sends terminal confidential information to RAM 113b for communication link keys.

[0066] Identification number decision equipment 140 is started in response to the starting command from card detection equipment 103b, chooses one of the center confidential information which nonvolatile memory 112b

holds, and sends the identification number to nonvolatile memory 112b and data output equipment 101b.

[0067] Here, the decision of an identification number may be made by random numbers, and you may carry out based on time information. Moreover, the identification number of single confidential information in which the operation whose nonvolatile memory 112b has only single confidential information is also possible, and nonvolatile memory 112b has identification number decision equipment 140 in this case will be outputted.

[0068] Although the example which carries out a communication link and writing as respectively independent equipment was shown here, the operation as one equipment which has the mode of a communication link and writing like the example of drawing 3 is also possible.

[0069] Drawing 6 is an example which carries out this invention by using an IC card as a terminal.

[0070] An output unit 200 sends Terminal ID to reception and a card reader 220 from the nonvolatile memory 210 for ID maintenance.

[0071] From a card reader 220, an input unit 201 writes reception and Terminal ID in the nonvolatile memory 210 for ID maintenance, and writes a terminal confidential information list for Terminal ID and a terminal confidential information list in the nonvolatile memory 211 for confidential information maintenance.

[0072] An input device 201 sends an output command for a data demand command to reception and the nonvolatile memory 210 for ID maintenance from a card reader 220 again. Further, an input unit 201 sends a terminal confidential information identification number to reception from a card reader 220, and sends this to the nonvolatile memory 211 for confidential information maintenance.

[0073] The nonvolatile memory 210 for ID maintenance carries out reception maintenance of the terminal ID from an input unit 201. The nonvolatile memory 210 for ID maintenance receives an output command from an input unit 201, and sends Terminal ID to an output unit 200 again.

[0074] The nonvolatile memory 211 for confidential information maintenance receives and holds a terminal confidential information list from an input unit 201. The nonvolatile memory 211 for confidential information maintenance sends a terminal confidential information identification number to reception from an input unit 201, and sends corresponding terminal confidential information to RAM212 for communication link keys again.

[0075] RAM212 for communication link keys carries out reception maintenance of the terminal confidential information from the nonvolatile memory 211 for confidential information maintenance.

[0076] RAM212 for communication link keys consists of equipment which performs the communication link with a card reader accessible.

[0077] Here, although the example carried out to the ATM card of a bank was described, it can carry out also like the PURIPEDO card used for large applications, such as a telephone and a means of transportation. Moreover, it can also carry out to the communication link between the IC card of the non-contact mold used with the ski lift etc., and tariff collection equipment.

[0078] Moreover, the operation to the approach of performing the communication link of a mounted terminal and road-side equipment for tariff collection of a highway is also possible. In this case, the user of a mounted terminal besides the operation which realizes a mounted terminal as a PURIPEDO card is registered, and the method of collecting a tariff later is also considered.

[0079]

[Effect of the Invention] By this invention, a center can perform secret communication with a terminal, and terminal authentication, without having a confidential information list of each terminals. Moreover, since it was possible to use a high-speed secret key cryptosystem and a high-speed Hash Function unlike key sharing of ID use, big computational complexity became unnecessary.

[Translation done.]

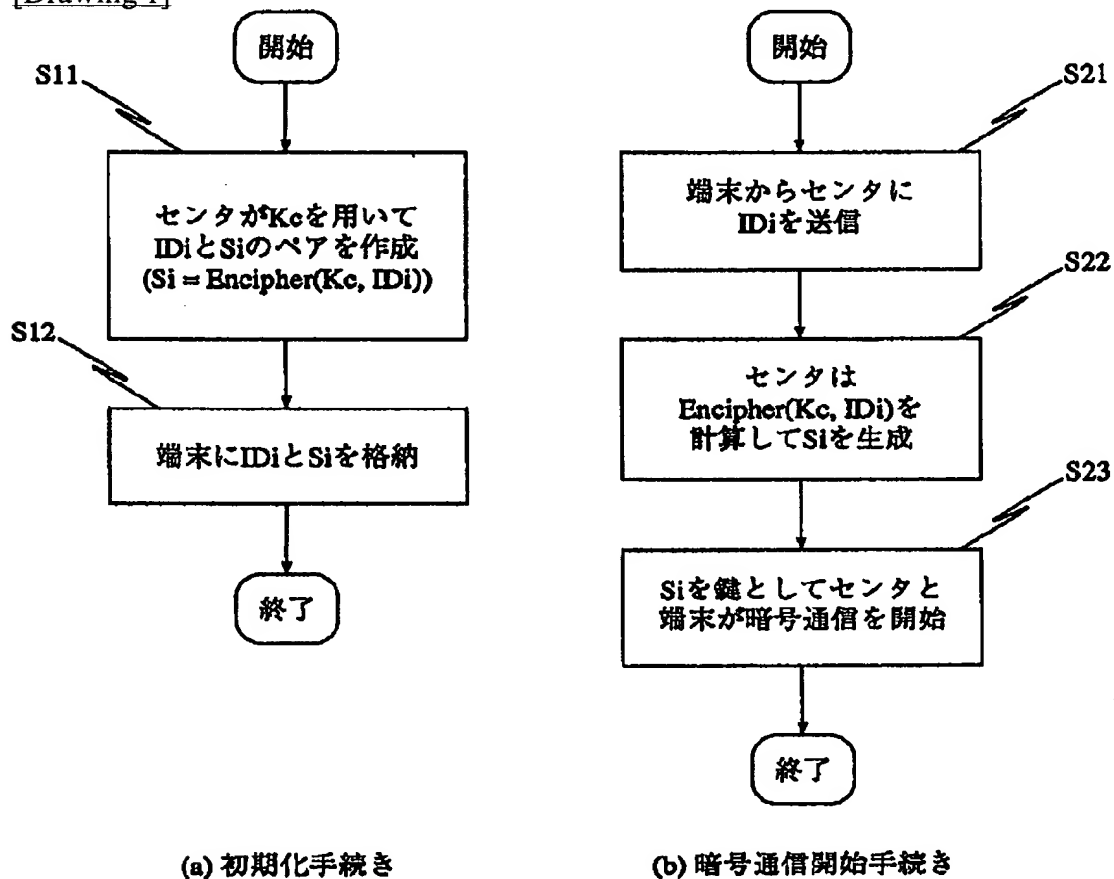
* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

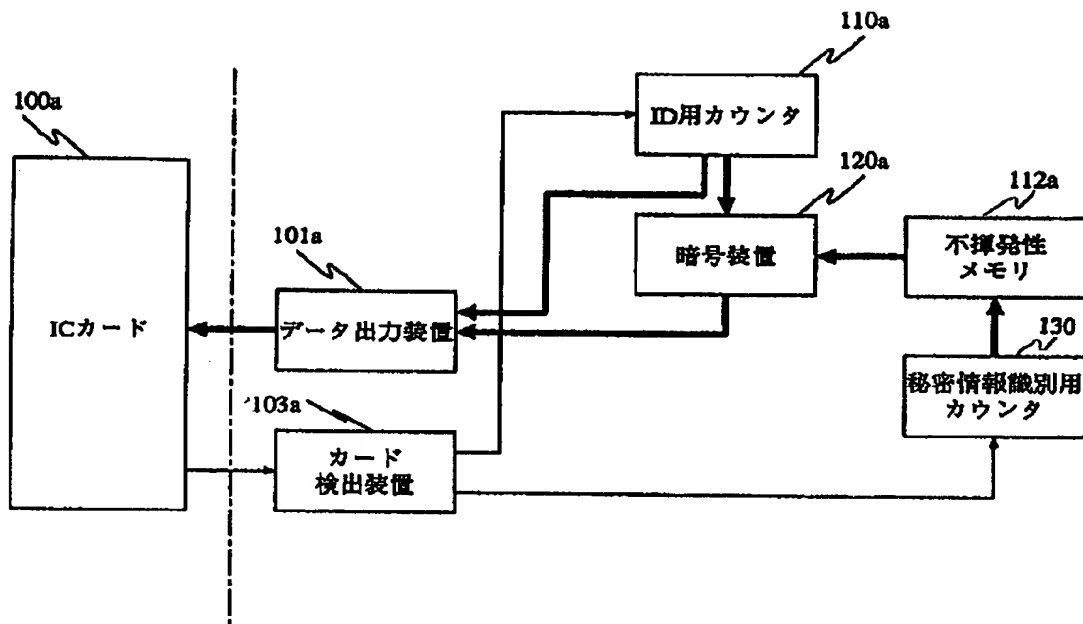
1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DRAWINGS

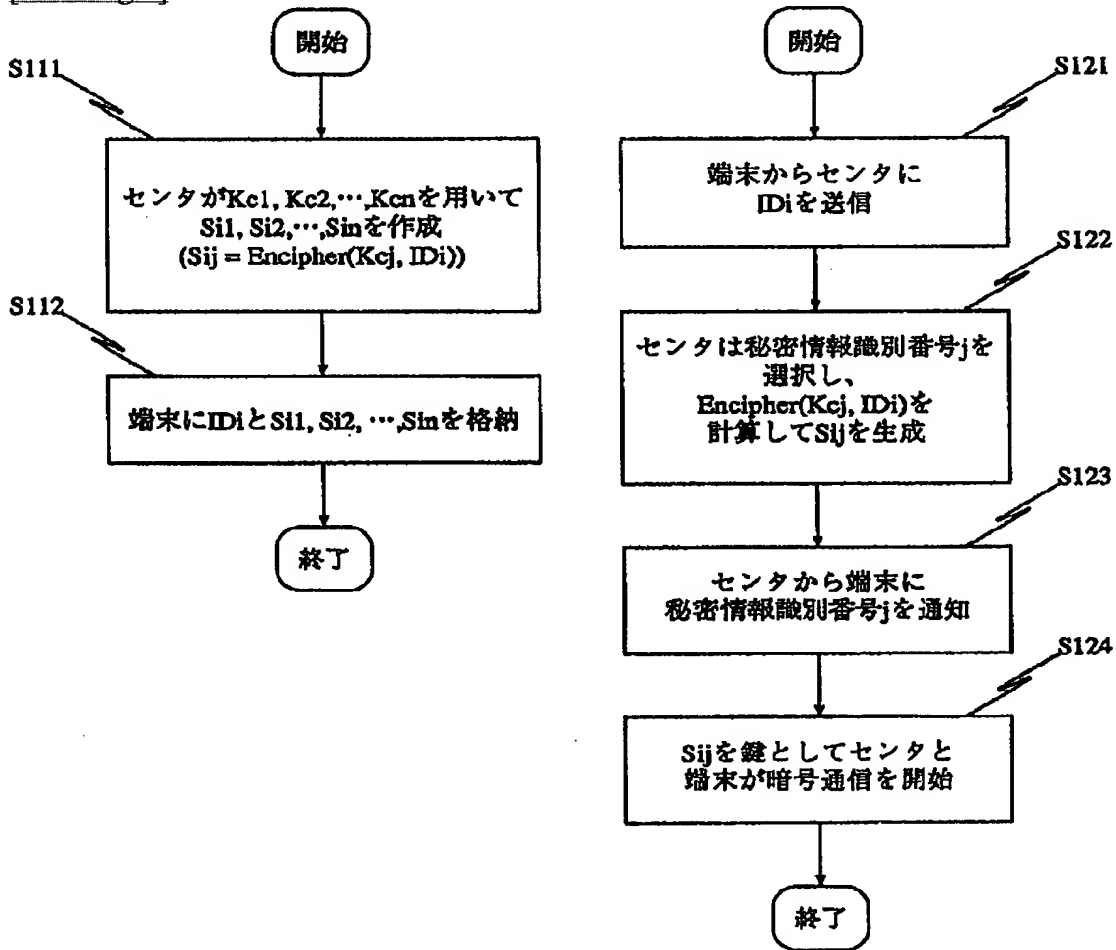
[Drawing 1]



[Drawing 4]



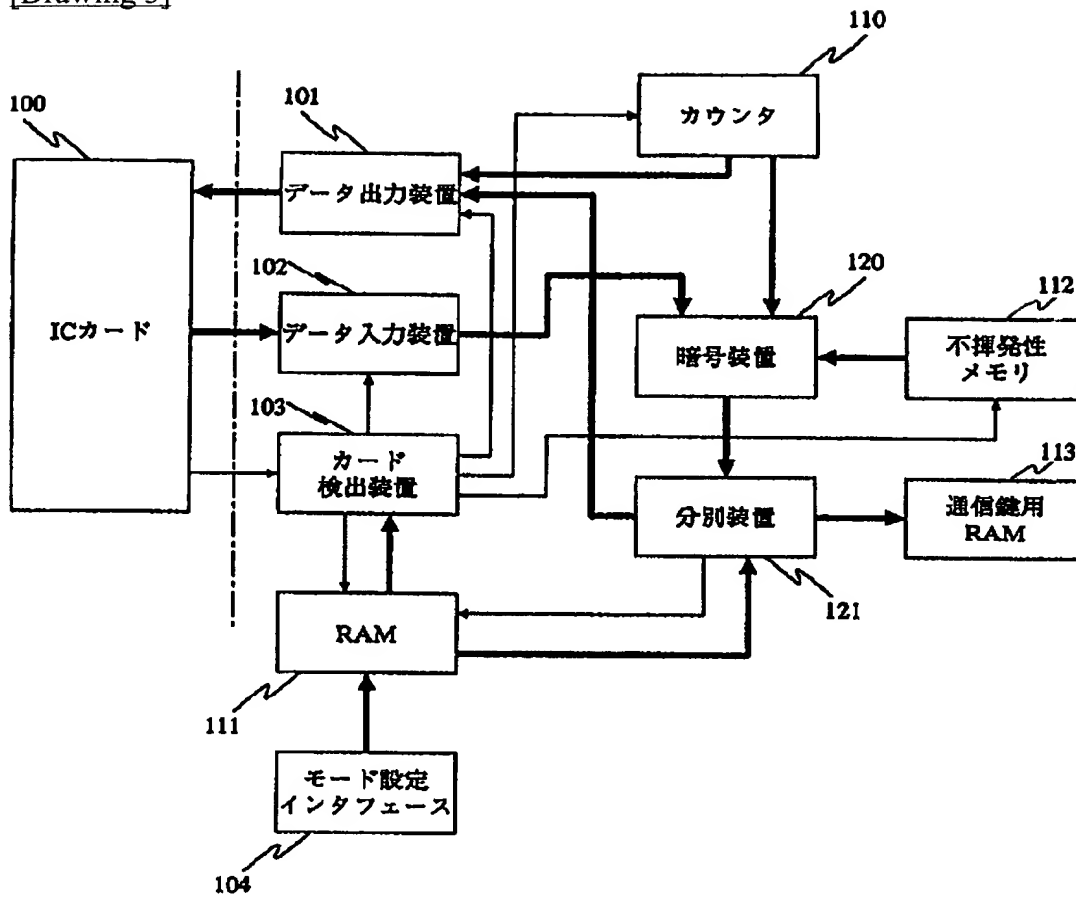
[Drawing 2]



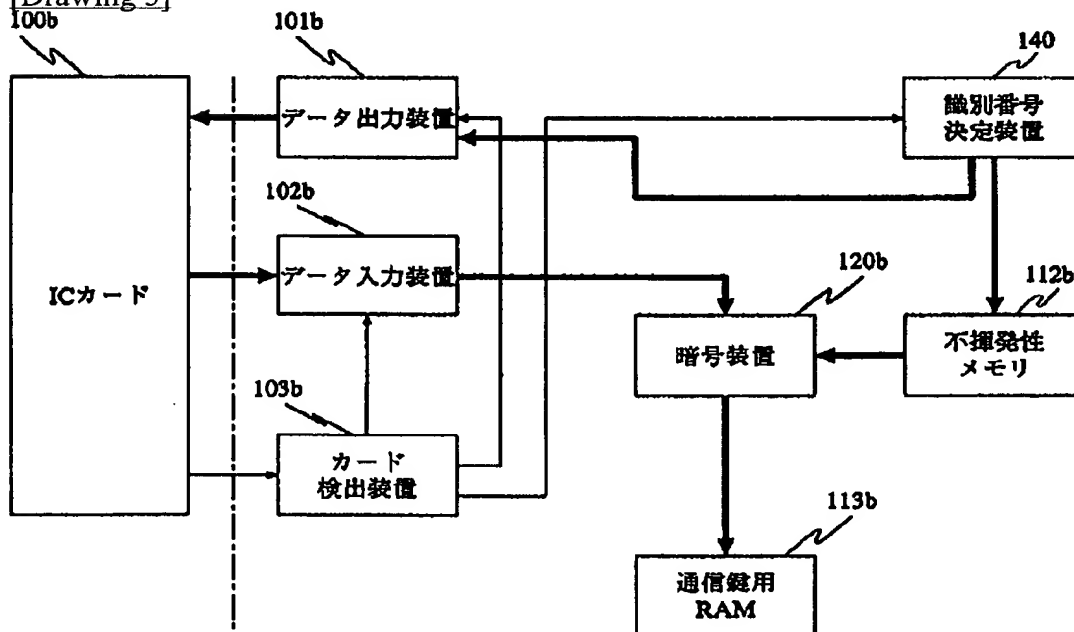
(a) 初期化手続き

(b) 暗号通信開始手続き

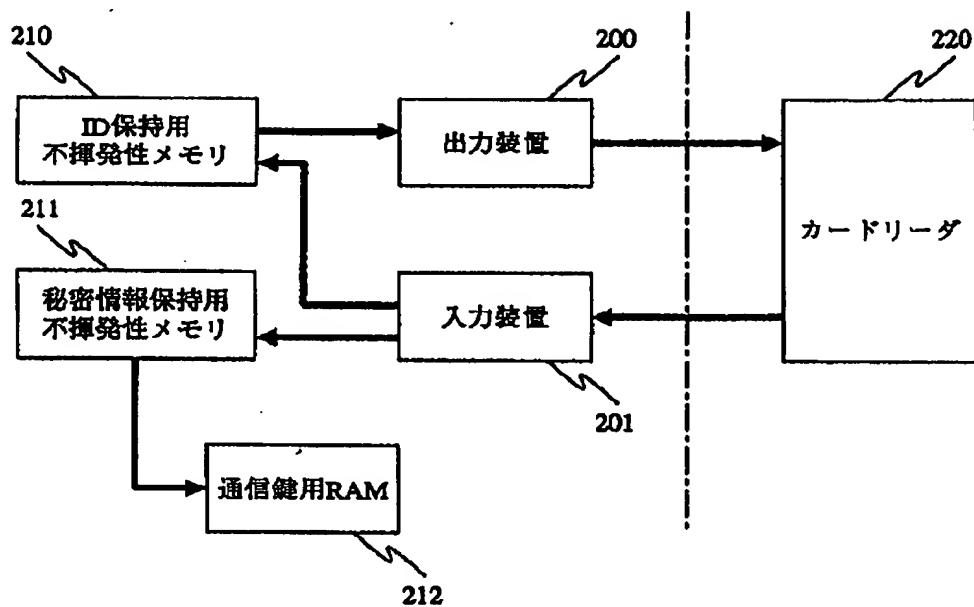
[Drawing 3]



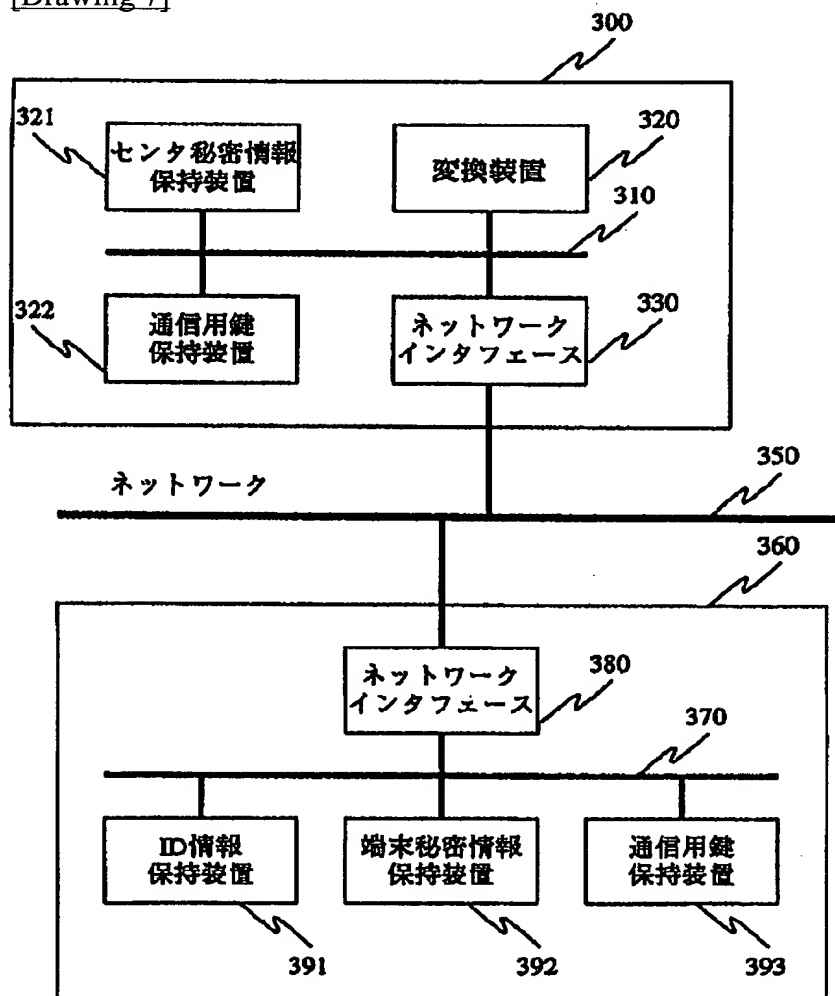
[Drawing 5]



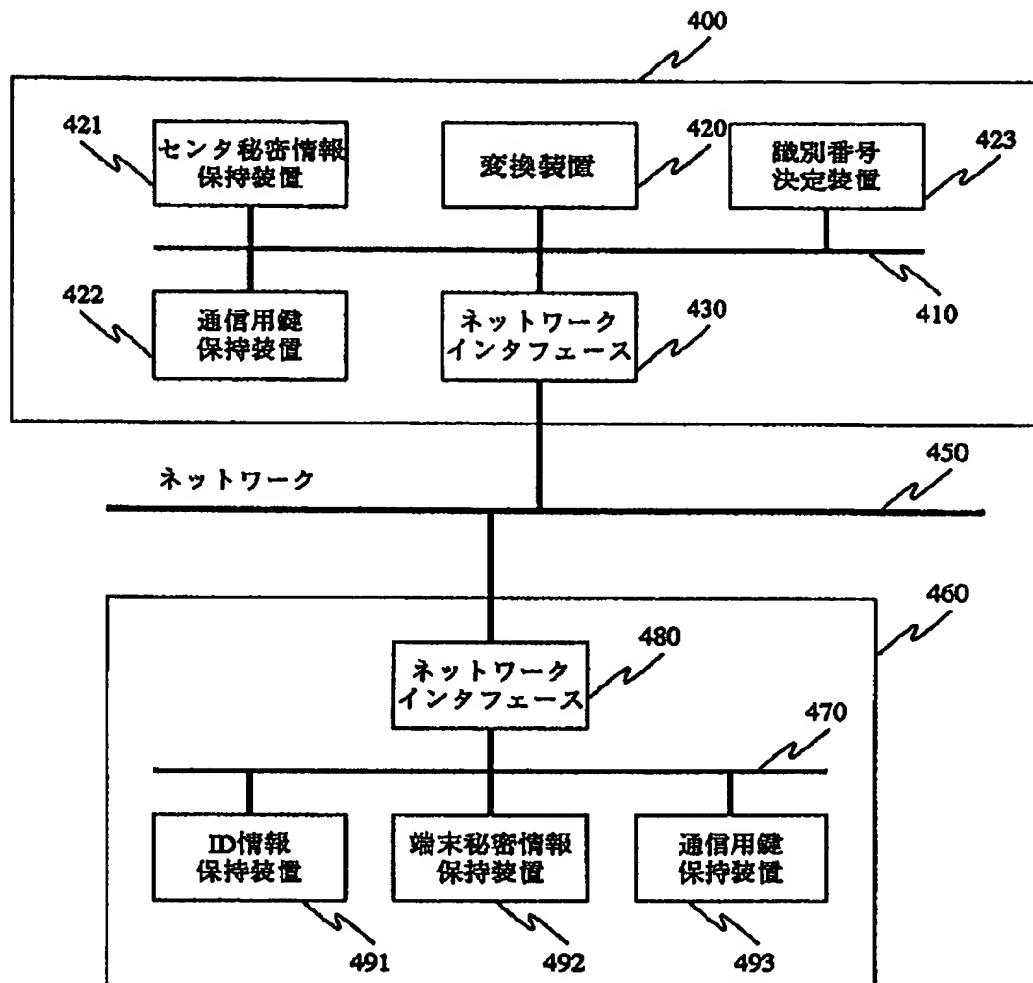
[Drawing 6]



[Drawing 7]



[Drawing 8]



[Translation done.]

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☐ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☐ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.